

AMENDMENTS TO THE CLAIMS:

This listing of claims will replace all prior versions and listings of claims in the application:

1. (Currently Amended) A computer-implemented method for authenticating an electronic message sent from a sender to a recipient, comprising the steps performed by a computer of:
 - receiving, at an authentication server, the electronic message from the sender, the electronic message comprising message data and an electronic mail address of the recipient;
 - creating a digest of the message data;
 - appending a temporal stamp and a unique value to the digest;
 - signing the digest, the temporal stamp, and the unique value with a digital signature;
 - sending, from the authentication server, to the recipient, the electronic message and an electronic postmark data structure comprising the digest, the temporal stamp, the unique value, and the digital signature to the electronic mail address, the electronic message being sent from the authentication server as data that is separate from the electronic postmark data structure as an electronic postmark data structure;
 - authenticating the digest, the temporal stamp, the unique value, and the digital signature;
 - storing, at the authentication server, a copy of the digest, the temporal stamp, the unique value, and the digital signature in a log file; and
 - creating a digest of the log file.

2. (Original) The method of claim 1, where the step of creating a digest comprises generating a one-way hash value from the electronic message.
3. (Original) The method of claim 1, wherein the step of creating a temporal stamp comprises using the time and the date which indicate when the electronic message was received.
4. (Previously Presented) The method of claim 1, wherein the step of sending the digest, the temporal stamp, the unique value, and the digital signature comprises sending the electronic message.
5. (Canceled)
6. (Original) The method of claim 4 wherein the step of sending the electronic message comprises attaching at least one legal protection of an official entity.
7. (Canceled)
8. (Previously Presented) The method of claim 1, further comprising the step of:
appending a temporal stamp to the digest of the log file; and
signing the digest of the log file and temporal stamp with a digital signature.
9. (Previously Presented) The method of claim 1 wherein the step of authenticating further comprises the steps of:
verifying that the digital signature was signed by the official entity;

verifying the specific identity of the entity which signed the digital signature; and
authenticating the message data using the digest.

10. (Currently Amended) A computer-implemented method for authenticating an electronic message sent from a sender to a recipient, comprising the steps performed by a computer of:

sending the electronic message from the sender to a sender client using an e-mail program, the electronic message comprising message data and an electronic mail address of the recipient;

receiving the electronic message at the sender client;

creating, by the sender client, a hash value from the message data;

sending the hash value and the recipient electronic address from the sender client to an authentication server;

generating an electronic postmark data structure by the authentication server, the electronic postmark data structure including the hash value, item and date information, and a value that uniquely identifies the electronic postmark data structure;

sending, from the authentication server, the electronic message and the electronic postmark data structure and the recipient electronic mail address from the authentication server to a recipient client, the electronic message being sent from the authentication server as data that is separate from the electronic postmark data structure;

sending the electronic message and the electronic postmark data structure from the recipient client to a recipient at the recipient electronic mail address;

authenticating the electronic postmark data structure at the recipient client;

storing, at the sender client, a copy of the electronic postmark data structure in a log file; and
creating a digest of the log file.

11. (Original) The method of claim 10, wherein the step of generating an electronic postmark data structure includes generating a digital signature for inclusion in the electronic postmark data structure.
12. (Original) The method of claim 11, wherein the step of generating a digital signature includes generating a digital key.
13. (Original) The method of claim 12, wherein the step of authenticating the electronic postmark data structure includes using the digital key.
14. (Original) The method of claim 11, wherein the step of generating a digital key involves including the digital key with the digital signature.
15. (Original) The method of claim 10, wherein the step of sending the hash value includes using an authentication server, which is an electronic postmark server.
16. - 19. (Cancelled)
20. (Currently Amended) A computer-implemented method for receiving authentication of an electronic message sent from a sender to a recipient, the authentication being performed by a receiver client, comprising the steps performed by a computer of:

receiving a recipient electronic mail address and an electronic postmark data structure for the electronic message sent by the sender to the recipient using an e-mail program from an authentication server, the electronic postmark data structure including time and date information and a value that uniquely identifies the electronic postmark data structure;

sending, from the authentication server, the electronic message and the electronic postmark data structure to the recipient at the recipient electronic mail address, the electronic message being sent sent from the authentication server as data that is separate from the electronic postmark data structure;

storing, at the authentication server, a copy of the electronic postmark data structure including time and date in a log file: and

creating a digest of the log file.

21. (Original) The method of claim 20, wherein the step of receiving the electronic message involves communicating between the receiver client and the authentication server using TCP/IP.
22. (Original) The method of claim 20, wherein the step of receiving the electronic message from an authentication server involves using the authentication server which is an electronic postmark server.
23. (Original) The method of claim 20, further comprising the step of: verifying the electronic postmark data structure using a digital key.

24. (Original) The method of claim 23, wherein the step of verifying the electronic postmark data structure involves including the digital key with the electronic postmark data structure.
25. (Original) The method of claim 20, wherein the step of receiving a recipient electronic address and an electronic postmark data structure further includes the step of receiving the electronic message.
26. (Original) The method of claim 20, wherein the step of sending the electronic postmark data structure to a recipient further includes the step of sending the electronic message.
27. - 46. (Cancelled)